IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

PLAINTIFF BRANDON HUYLER, on behalf of himself and on behalf of all others similarly situated, Plaintiff, v. AT&T, INC., Defendant.	Case No.: 3:24-cv-00847 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Brandon Huyler, by his undersigned counsel, files this Class Action Complaint individually and on behalf a class of all similarly situated persons against AT&T, Inc. ("Defendant" or "AT&T"). Plaintiff bases the following allegations on personal knowledge, due investigation of counsel, and, where indicated, on information and belief, and states the following:

NATURE OF THE ACTION

1. Defendant describes itself as a leading provider of wireless and wireline telecom and broadband services to consumers in the United States and businesses globally.[1] In the United States, its network covers over 334 million people with LTE technology and over 302 million people with 5G technology.[2] AT&T also has more than 8.3 million fiber consumers.[3]

2. As a major provider of telephone and internet services to the United States population, AT&T understood it had the duty and responsibility to protect customers' information

[1] AT&T Inc., Form 10-K, U.S. Sec. Exch. Comm'n (February 23, 2024), https://www.sec.gov/ix?doc=/Archives/edgar/data/732717/000073271724000009/t-20231231.htm (last accessed April 4, 2024).
[2] *Id.*
[3] *Id.*

that it collected, stored, and maintained, expressly advertising to potential customers that "we work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment."[4] Defendant failed to meet its duty and, as a direct result, millions of customers' sensitive information with which it was entrusted was released, stolen, and made publicly available on the dark web.

3. On March 30, 2023, in a blog post on its website, Defendant announced that unauthorized threat actors had accessed approximately 73 million of its former and current customers' accounts without authorization and compiled the information into a data set ("Data Set") that was released on the dark web (the "Data Breach").[5]

4. The sensitive personally identifying information ("PII") released to the threat actor included millions of individuals' private information including, *inter alia*, customers' full names, email addresses, mailing addresses, phone numbers, dates of birth, social security numbers, AT&T account numbers, and passcodes.

5. Worse yet, this Data Set was also made available publicly on the open web. The forum where the leaked data appeared was accessible with a regular internet browser— no special software or special networks were required, as is often the case with leaked data appearing on the dark web. The Data Set is "easily discoverable via a Google search and immediately shows many PII […] records from the AT&T breach."[6]

---

[4] *AT&T Privacy Notice*, AT&T https://about.att.com/privacy/privacy-notice.html (last accessed April 4, 2024).

[5] *Keeping Your Account Secure* ("Notice"), AT&T (updated April 3, 2024), https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last accessed April 4, 2024).

[6] Jon Brodkin, *AT&T acknowledges data leak that hit 73 million current and former users*, ARS Technica, https://arstechnica.com/tech-policy/2024/04/att-acknowledges-data-leak-that-hit-73-million-current-and-former-users/ (last accessed April 4, 2024).

6. In order to obtain Defendant's services, individuals must entrust AT&T with sensitive, private information. Defendant requires this information in order to perform its regular business activities.

7. Since the Data Breach occurred, several news sources have reported that threat actors released the Data Set containing all of the stolen data on the dark web.[7] Defendant has failed to acknowledge the unauthorized access of its customers' data until now, despite the unauthorized access of information in the Data Set being reported as early as August of 2021 and has failed to inform victims exactly when and how the Data Breach occurred.

8. As a direct and proximate result of Defendant's inadequate data security measures, and its breach of its duty to handle PII with reasonable care, Plaintiff's and Class Members' PII have been accessed by hackers and exposed to an untold number of unauthorized individuals.

9. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiff, on behalf of himself, and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of an implied contract, unjust enrichment, and declaratory

[7] *See e.g.*, Chloe Veltman, *Millions of customers' data found on dark web in latest AT&T data breach*, Nat. Pub. Radio (March 30, 2024), https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web (last accessed April 4, 2024); Aimee Ortiz, *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, The New York Times (March 30, 2024), https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html (last accessed April 4, 2024).

judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

12. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

PARTIES

14. Plaintiff Brandon Huyler is an adult, who at all relevant times, is and was a citizen and resident of the State of Illinois. Plaintiff is a customer of AT&T who received a notice from Defendant, informing him that his PII provided to Defendant had been compromised in the Data Breach.

15. Since the unauthorized access of information in the Data Set, Plaintiff has suffered emotional distress as a result of his PII being accessed and exposed to unauthorized third parties.

16. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

17. AT&T, Inc., is a corporation organized under the laws of Delaware and maintains its headquarters and principal place of business at 208 S. Akard St. Dallas, TX 75202. Defendant's registered agent for service of process is CT Corporation System, which maintains offices located at 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

FACTUAL BACKGROUND

A. Defendant Collected Plaintiff's and Class Members' PII as a Necessary Part of Its Routine Business Dealings with Them.

18. AT&T is a self-described leading provider of wireless and wireline telecom and broadband services to consumers in the United States and businesses globally.[8] In the United States, its network covers over 334 million people with LTE technology and over 302 million people with 5G technology.[9] AT&T also has more than 8.3 million fiber consumers.[10] For the fiscal year ending December 31, 2023, AT&T reported operating income of approximately $23.5 billion.[11]

19. As a condition of receiving AT&T's telecommunication services, customers must provide it with sensitive PII, which includes, upon information and belief, full names, addresses, phone numbers, social security numbers, and account information.

20. AT&T derives substantial benefit from this information because, but for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its various services.

21. AT&T acknowledges the vast amounts of PII with which it is entrusted and claims:

---

[8] AT&T Inc., Form 10-K, U.S. Sec. Exch. Comm'n (February 23, 2024), https://www.sec.gov/ix?doc=/Archives/edgar/data/732717/000073271724000009/t-20231231.htm

[9] *Id.*

[10] *Id.*

[11] *Id.*

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[12]

22. AT&T also touts its cybersecurity risk management strategy, stating:

> We maintain a network and information security program that is reasonably designed to protect our information, and that of our customers, from unauthorized risks to their confidentiality, integrity, or availability. Our program encompasses the CSO and its policies, platforms, procedures, and processes for assessing, identifying, and managing risks from cybersecurity threats, including third-party risk from vendors and suppliers; and the program is generally designed to identify and respond to security incidents and threats in a timely manner to minimize the loss or compromise of information assets and to facilitate incident resolution.
>
> We maintain continuous and near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. This security monitoring leverages tools, where available, such as near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trend analysis and predictive security alerting. We assess, identify, and manage risks from cybersecurity threats through various mechanisms, which from time to time may include tabletop exercises to test our preparedness and incident response process, business unit assessments, control gap analyses, threat modeling, impact analyses, internal audits, external audits, penetration tests and engaging third parties to conduct analyses of our information security program. We conduct vulnerability testing and assess identified vulnerabilities for severity, the potential impact to AT&T and our customers, and likelihood of occurrence. We regularly evaluate security controls to maintain their functionality in accordance with security policy. We also obtain cybersecurity threat intelligence from recognized forums, third parties, and other sources as part of our risk assessment process. In addition, as a critical infrastructure entity, we collaborate with numerous agencies in the U.S. government to help protect U.S. communications networks and critical infrastructure, which, in turn, informs our cybersecurity threat intelligence.[13]

---

[12] *AT&T Privacy Notice*, AT&T https://about.att.com/privacy/privacy-notice.html (last accessed April 4, 2024).

[13] AT&T Inc., Form 10-K, U.S. Sec. Exch. Comm'n (February 23, 2024), https://www.sec.gov/ix?doc=/Archives/edgar/data/732717/000073271724000009/t-20231231.htm.

23. Plaintiff and Class Members directly or indirectly entrusted AT&T with their sensitive and confidential PII and therefore reasonably expected that Defendant would safeguard their highly sensitive PII and keep it confidential.

24. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, AT&T assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

25. Despite these duties, AT&T failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and ultimately allowed nefarious third-party hackers to breach its computer systems, compromising Plaintiff's and Class Members' PII stored therein.

B. AT&T Knew the Risks of Storing Valuable PII and the Foreseeable Risk of Harm to Victims.

26. AT&T was well aware that the PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

27. AT&T also knew that a breach of its computer systems, and release of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private information.

28. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

29. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft and medical and financial fraud.[14] Indeed, a robust "cyber black market" exists in which criminals openly post

[14] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed April 4, 2024).

stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

30. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available. Indeed, the information compromised during the Data Breach has already been released on the internet.

31. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2023, there were 3,205 data compromises affecting 353 million individuals, which set a record high number of data compromises in the U.S. in a single year, representing a 72% increase from the previous all-time high number of comprises set in 2021.[15]

32. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, approximately 650,000 people reported identity fraud compared to over a million people in 2023, representing an increase of approximately 19%.[16]

33. The breath of data compromised makes the information particularly vulnerable to thieves and leaves AT&T's customers especially vulnerable to fraud and other risks.

[15] *Facts + Statistics; Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last accessed April 4, 2024).
[16] *Id.*

34. The ramifications of AT&T's failure to keep Plaintiff and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

35. Further, a data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[17]

36. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

37. Moreover, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, information such as social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of

[17] Erika Harrell, Bureau of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed April 4, 2024).

the person's relationships with government agencies and any number of private companies to update the person's accounts with those entities.

38. The Social Security Administration even warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[18]

39. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

40. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more

[18] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 4, 2024).

sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[19]

41. In light of high-profile data breaches at other companies, AT&T knew or should have known that its computer systems would be targeted by cybercriminals.

42. Defendant also knew or should have known the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers' PII from occurring.

C. Defendant Released Highly Sensitive PII to Hackers and Breached its Duty to Protect Customer PII.

43. On March 30, 2024, AT&T posted a notice ("Notice") on its website regarding the Data Breach in an article euphemistically titled "Keeping your account secure."[20]

44. Defendant's Notice advised, in part, that AT&T learned of unauthorized access to its computer systems impacting 7.6 million current AT&T customers and 65.4 million former account holders. Leaked information included full names, email addresses, mailing address, phone number, social security number, date of birth, AT&T account number, and passcode.

45. The Notice did not disclose when the unauthorized intrusion occurred or when Defendant learned that the information had been released. Further, the Notice stated that Defendant was still unaware of unauthorized access to its systems pertaining to the leaked PII.

46. Unauthorized access of information in the Data Set was first reported in August 2021, when ShinyHunters, a known threat actor, offered the information for sale on the dark web

[19] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed April 4, 2024).
[20] Notice, *supra* note 5.

with a "buy it now" price of one million dollars.[21] AT&T stated in response that, "based on [its] investigation today, the information […] does not appear to have come from our systems" and refused to confirm whether the customer information was valid.[22]

47. On or about March 17, 2024, a different threat actor released the Data Set on public and Tor versions of a hacking forum.[23] Viewing the AT&T data requires a hacking forum account and site "credits" that can be purchased or earned by posting on the forum.[24]

48. Importantly, AT&T's Notice describing the Data Set as being released on the dark web is incorrect and misleading. Security researcher Troy Hunt wrote that the data is "out there in plain sight on a public forum easily accessed by a normal web browser."[25] He explained that the term "dark web" is "incorrect and misleading" in this case:

> No special software, no special network, just a plain old browser. It's easily discoverable via a Google search and immediately shows many PII […] records from the AT&T breach. Registration is then free for anyone with the only remaining barrier being obtaining credits.[26]

49. This distinction is important, as Troy Hunt explained, "there's only one thing worse than your data appearing on the dark web: it's appearing on the clear web. And that's precisely where it is; the forum this was posted to isn't within the shady underbelly of a Tor hidden service,

---

[21] *See* Jon Brodkin, *AT&T acknowledges data leak that hit 73 million current and former users*, ARS Technica, https://arstechnica.com/tech-policy/2024/04/att-acknowledges-data-leak-that-hit-73-million-current-and-former-users/ (last accessed April 4, 2024).
[22] Lawrence Abrams, *AT&T denies data breach after hacker auctions 70 million user database*, Bleeping Computer (August 20, 2021), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/ (last accessed April 4, 2024).
[23] Jon Brodkin, *AT&T acknowledges data leak that hit 73 million current and former users*, ARS Technica, https://arstechnica.com/tech-policy/2024/04/att-acknowledges-data-leak-that-hit-73-million-current-and-former-users/ (last accessed April 4, 2024).
[24] *Id*.
[25] *Id*.
[26] *Id*.

it's out there in plain sight on a public forum easily accessed by a normal web browser. And the data is real."[27]

50. On or about March 30, 2024, Defendant finally began notifying customers that it had preliminarily determined that their PII was compromised. AT&T delivered a data breach notification email to Plaintiff and Class Members, alerting them that their PII had been leaked on the internet.

51. In sum, upon information and belief, as a result of Defendant's failure to implement adequate data security measures, Plaintiff's and Class Members' PII, was negligently released to unauthorized, malicious threat actors and is now at risk of dissemination and use by other unauthorized individuals or cybercrime groups.

D. Defendant Failed to Comply with FTC Guidelines.

52. AT&T is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

53. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

---

[27] Troy Hunt, *Inside the Massive Alleged AT&T Data Breach* (March 19, 2024), https://www.troyhunt.com/inside-the-massive-alleged-att-data-breach/ (last accessed April 4, 2024).

[28] *Start with Security: A Guide for Business*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed April 4, 2024).

54. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures, including:[29]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the

[29] *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed April 4, 2024).

network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. Upon information and belief, AT&T failed to properly implement one or more of the basic data security practices described above. AT&T's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized release of Plaintiff's and Class Members' PII to a nefarious threat actor. Further, AT&T's failure to implement basic data security practices constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

57. AT&T was at all times fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. AT&T was also aware of the significant repercussions that would result from its failure to do so.

58. AT&T's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff and Members of the Class Have Suffered Concrete Injury.

59. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff, and members of the Class, significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

60. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

61. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII.

62. In 2021 alone, identity theft victims in the United States had financial losses totaling $16.4 billion.[30]

63. Besides the monetary damage sustained, consumers may also spend anywhere from one day to more than six months resolving identity theft issues.[31]

64. Ultimately, the time that victims spend monitoring and resolving identity theft issues takes an emotional toll. Approximately 80% of victims of identity theft experienced some type of emotional distress, and more than one-third of victims experienced moderate or severe emotional distress.[32]

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

66. As a result of AT&T's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their highly valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further

[30] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, U.S. Dept. Just., Bureau Just. Stats. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf (last accessed April 4, 2024).
[31] *Supra* note 35.
[32] *Id.*

breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII with which it was entrusted.

F. Plaintiff and Members of the Class Are Now at an Increased Risk of Future Harms.

67. Data Breaches such as the one experienced by Plaintiff and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

68. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[33] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiff and Class Members) must take after a Data Breach like AT&T's are both time-consuming and of only limited and short-term effectiveness.

69. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

70. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove

---

[33] Government Accountability Off., "Data Breaches" (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last accessed April 4, 2024).

[34] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," Government Accountability Off. (June 2007), https://www.gao.gov/new.items/d07737.pdf ("2007 GAO Report") (last accessed April 4, 2024).

fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

71. Theft of PII is also gravely serious as PII is a valuable property right.[36]

72. There may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[37]

73. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

74. Because the entirety of the stolen information has *already* been released on the dark web, every Class Member, including Plaintiff, is at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

G. Plaintiff's Experience.

75. Plaintiff has been an AT&T customer since at least February 2018. In connection with the registration of Plaintiff's account, Plaintiff was required to provide his PII to AT&T in exchange for AT&T's services, including, *inter alia*: his full name, email address, mailing address,

---

[35] *See* Identity Theft Victim Checklist, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last accessed April 4, 2024).
[36] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("SPI") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("SPI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[37] *See* 2007 GAO Report, at 29.

phone number, date of birth, social security number, and account information, including his passcode. When providing Defendant with his PII, Plaintiff expected that his PII would be kept confidential.

76. On or about March 30, 2023, Plaintiff received an email from AT&T informing Plaintiff that the PII he provided to Defendant had been compromised during the Data Breach. Plaintiff did not consent to Defendant's release of his PII to threat actors.

77. Since the Data Breach, Plaintiff has spent numerous hours taking action to mitigate the impact of the Data Breach, which included additional review and monitoring of his personal and financial accounts, endeavoring to implement additional security measures where appropriate, and researching credit card monitoring services. Plaintiff took these mitigation efforts and incurred this loss of time as a direct and proximate result of the Data Breach.

78. Knowing that a threat actor stole his PII and made it freely available on the internet has caused Plaintiff anxiety. He is now very concerned about identity theft and impending privacy harms arising from the Data Breach. Plaintiff further has concerns of Defendant suffering future data breaches or otherwise releasing Plaintiff's PII in the future.

79. Plaintiff has suffered actual injury from having his PII exposed as a result of the Data Breach, including, but not limited to: (a) paying monies to AT&T for its services Plaintiff would not have purchased had it disclosed that it lacked data security practices to safeguard its customers' PII from theft; (b) damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to AT&T; (c) loss of privacy; (d) lost time; and (e) imminent and impending injury arising from the increased risk of fraud and identity theft.

80. As a result of the Data Breach, Plaintiff will continue to be at a heightened risk for identity theft and attendant damages for years to come.

CLASS ALLEGATIONS

81. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose PII was compromised in the AT&T Data Breach announced on March 30, 2024 (the "Class").

82. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

83. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

84. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Defendant has not stated the number of individuals implicated in the Data Breach, but the number is reportedly in the millions.

85. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

c. Whether Defendant obtained Plaintiff's and Class Members' PII;

d. Whether Defendant released Plaintiff's and Class members' PII without authorization;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately and timely responded to the Data Breach;

g. Whether Defendant failed to maintain reasonable security systems and procedures, including those required by applicable security laws and regulations and those consistent with industry standards;

h. Whether Defendant remedied the vulnerabilities that permitted the Data Breach to occur;

i. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or other equitable relief as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

86. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard their PII. Plaintiff and Class Members entrusted Defendant with their PII, and it was subsequently released to an unauthorized third party and made publicly available on the internet.

87. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members Plaintiff seek to represent; Plaintiff has retained counsel competent and experienced in complex class action

litigation and data breach litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

88. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

89. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty and released Plaintiff's and Class Members' PII, then Plaintiff and each Class member suffered damages by that conduct.

90. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiff and the Class)

91. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

92. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

93. AT&T's duty to use reasonable care arose from several sources, including but not limited to those described below.

94. Defendant has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By receiving, maintaining, and handling PII that is routinely targeted by criminals for unauthorized access, AT&T was obligated to act with reasonable care to protect against these foreseeable threats.

95. AT&T breached the duties owed to Plaintiff and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor

the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

96. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, its PII would not have been compromised.

97. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

98. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(Plaintiff on Behalf of the Class)

99. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of AT&T's duty.

101. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving the PII it entrusted from its customers.

102. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

103. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act is intended to guard against.

105. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiff on Behalf of the Class)

107. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

108. Plaintiff brings this claim individually and on behalf of the Class.

109. When Plaintiff and members of the Class provided their PII to Defendant in exchange for its services, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiff's and Class Members' PII, comply with their statutory and common law duties to protect Plaintiff's and Class Members' PII, and to timely notify them in the event of a data breach.

110. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's provision of internet and phone services. Plaintiff and Class Members accepted Defendant's offers when they made and paid for purchases of Defendant's services and provided their PII to Defendant.

111. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with their statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

112. Defendant's implied promise to safeguard customer PII is evidenced by, *e.g.*, the representations in Defendant's privacy notice and other statements made by Defendant concerning its cybersecurity measures, as set forth in part *supra.*

113. Plaintiff and Class Members paid money to Defendant in order to receive telecommunication services. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

114. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised.

115. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

116. Defendant breached its implied contract with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII.

117. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

118. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiff on Behalf of the Class)

119. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

120. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Plaintiff's Breach of Implied Contract claim.

121. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

122. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known only to Defendant.

123. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased telecommunication services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

124. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

125. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

126. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

127. Defendant failed to secure Plaintiff and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

128. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

129. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

130. Plaintiff and Class Members have no adequate remedy at law.

131. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have sustained injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers likely to have criminal intentions and now have prime opportunities to

commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

132. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered damages and will continue to suffer other forms of injury and/or harm.

133. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiff on Behalf of the Class)

134. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

135. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

136. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether AT&T is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that AT&T's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

137. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed a legal duty to secure customers PII under the common law and Section 5 of the FTC Act; and

b. Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

138. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' PII.

139. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at AT&T. The risk of another such breach is real, immediate, and substantial. If another breach at AT&T occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

140. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

141. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AT&T, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and customers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: April 5, 2024

Respectfully submitted,

/s/ Bruce W. Steckler

Bruce W. Steckler, TX Bar No. 00785039
STECKLER WAYNE & LOVE, PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Tel: (972) 387-4040
Fax: (972) 387-4041

bruce@swclaw.com

Jonathan M. Jagher*
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
610.234.6486
jjagher@fklmlaw.com

Douglas A. Millen*
Nicholas R. Lange*
FREED KANNER LONDON & MILLEN LLC
100 Tri-State International Drive, Suite 128
Lincolnshire, IL 60629
224.632.4500
nlange@fklmlaw.com
dmillen@fklmlaw.com

**pro hac vice forthcoming*